Statement by

Robert F. Lentz

Director, Information Assurance

Assistant Secretary of Defense for

Networks and Information Integration

Before the

House Government Reform Committee

Hearing on

Information Security and

Implementation of the Federal Information Security Management Act of 2002

March 16, 2006

For Official Use Only

Until Release by the

Committee on Government Reform

U.S. House of Representatives

Thank you, Mr. Chairman and distinguished members of the Committee for this opportunity to testify before your Committee on Government Reform on the subject of Information Security and the Department of Defense's implementation of the Federal Information Security Management Act (FISMA) of 2002. I am Robert Lentz and this is my first opportunity to appear before you as the DoD Senior Information Assurance Officer. My prepared remarks cover the status of DoD's information security program and implementation of FISMA in the challenging cyber threat environment of the 21st Century.

To respond to this increased pace of cyber threats, technological change and evolving operational demands, the Department has integrated multiple programs and initiatives into an overarching approach protecting DoD information. DoD is leveraging the congressional reporting requirements under FISMA as a principal management and assessment tool to monitor and improve its IT security posture.

The Secretary of Defense's guidance has been that the protection of information and networks is fundamental to ensuring the success of warfare today. He has also emphasized that our adversaries have not been idle. Most of them know that they cannot defeat the United States military on a conventional battlefield, so they see cyber attacks as an inexpensive means of leveling that battlefield. These asymmetrical threats are real and the results of insecurity are potentially catastrophic.

To enable the transformation needed to meet the challenges posed by today's new threat environment, the Department's vision is of a single, secure grid providing seamless end-to-end information exchange capabilities to all warfighers, policy-makers, and support personnel that we call the Global Information Grid (GIG). The Department is leveraging emerging information technology to create this seamless, interoperable, network-centric environment. To translate that information technology into combat power, the Department is translating information technology into combat power and is migrating from platform-dependent to network-centric operations.

We must protect our information from threats: enemy, criminal, insider, or self-inflicted accidental events that weaken our security. Our information base and our ability to leverage the technology to support warfighting, intelligence, and business functions must have the highest level of trust and confidence or we lose the advantage that information provides us.

The GIG is a network of unprecedented complexity. It crosses organizational boundaries internal and external to the Department of Defense. The GIG is composed of an extensive variety of computers, communications hardware, and vast numbers of ancillary equipment. The responsibility for managing and operating these technologies and hardware extends across many DoD organizations and into many of our commercial partners.

The protection of the GIG is everyone's business - this cannot be overstated. We take specific actions to train, license, qualify, and certify pilots and weapons systems operators to a very high standard - we must consider no less of a standard for those who

operate, and ensure the security and integrity of the GIG. "Fighting the Net" is the commanders' business, but "Protecting the Net" is everyone's business.

Meeting Challenges

Our objective is to support defense and national security requirements through all levels of conflict and contingency support. Network-centric operations bring together joint, high-capacity networked operations and weapons systems, merging key tactical and strategic functional capabilities. The GIG supports all DoD missions, including joint and combined task-force commands, with the most effective, assured, and secure information-handling capabilities possible.

The Department's vision is to foster an agile, robust, interoperable and collaborative environment, where warfighters, business, and intelligence users all share knowledge in a secure, dependable and global net-centric environment that enables informed decision-making and effective operations. We will empower individuals at the edge of the network by providing them immediate access to information, and incorporating the information they provide into the GIG, while exploiting the weaknesses of enemies who are denied a comparable advantage. As part of DoD's information age transformation, the network is emerging as the most important contributor to combat power and force protection.

The DoD IA Strategic Plan

Because DoD is so large and complex, a comprehensive IA Strategic Plan is necessary to present an integrated view and consistent approach to security across the enterprise. The DoD IA Strategic Plan serves as the IA planning and management guide

for all Combatant Commands, Services, and Defense agencies. It establishes the Department's IA goals, sets out strategic objectives for IA, and provides a consistent approach to assuring information across the DoD enterprise and complying with FISMA. The IA Strategic Plan has five goals:

- Protect information to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed, at the client, within the enclave, at the enclave boundary, and within the computing environment, to ensure that all information has a level of trust commensurate with mission needs.
- Defend systems and networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and that all systems and networks are capable of self-defense.
- Provide integrated IA situational awareness/IA Command and Control (C2), integrating the IA posture into a user-defined operational picture (UDOP) synchronized with network operations (NETOPS) and emerging Joint C2 programs to provide decision makers and network operators at all command levels the tools for conducting Information Assurance/Computer Network Defense operations in net-centric warfare.
- Transform and enable IA capabilities innovatively by discovering emerging technologies, experimentation, and refining the development, delivery, and deployment processes to improve cycle time, reduce risk exposure, and increase return on investments.

- Create an IA-empowered workforce that is well equipped to support the changing demands of the IA/IT enterprise.

The DoD IA Policy Framework

The Department has developed an IA policy framework that provides overarching IA policy and procedural guidance to implement the IA Strategic Plan. The capstone Department of Defense Directive (DoDD) 8500.1, *Information Assurance*, was issued in October 2002. DoD Instruction (DoDI) 8500.2, *Information Assurance Implementation*, was issued in February 2003. Since then, additional policies that provide more detailed guidance on specific functional areas have been issued. They include such topics as computer network defense, certification and accreditation of all DoD systems, training and certification of the IA workforce, the DoD public key infrastructure, integrating IA into defense acquisition, IA for space systems, and biometrics.

Areas of Significant Improvement

The DoD has taken significant steps to address new threats and shortcomings in the defense of the GIG. Initiatives include:

Enterprise Solutions - The Department is aggressively pursuing prioritized enterprise solutions through centralized funding across all agencies, accelerating the implementation and closure of capability gaps. The Department has an effective defensive posture against cyber attacks. The Department selects and implements enterprise-wide computer network defense tools that automatically identify and remediate vulnerabilities, detect anomalies, mitigate insider threats,

and eliminates spyware. A number of additional products are being provisioned for enterprise deployment.

Configuration Management - The Department has comprehensive policies and processes for system configuration. One example is the distribution by the Air Force of Microsoft software with standard security configurations service-wide, resulting in improved network security and management The Department is aggressively moving toward a standard configuration management process similar to the successful efforts of the Air Force. As this concept proves itself over time, the Department will assess and may adopt similar processes for the enterprise.

The DoD has robust policies and processes for system configuration. The Defense Information System Agency (DISA) Field Security Operations develops Security Technical Implementation Guides (STIGs) for critical IT products. The DISA STIGs provide security configuration guidance for Windows NT, 2000, and 2003; UNIX (includes Solaris, HP-UX, and Linux); Database (includes Oracle and SQL Server); Network Infrastructure (includes Cisco IOS and Juniper IOS); and many other technologies such as OS/390, Web Servers (IIS, Netscape), Voice over Internet Protocol, Biometrics, Domain Name Server (DNS), Unisys, and Tandem.

Another aid to the standard configuration of machines by DoD is a DISA-developed product known as the "Gold Disk," which is based on the STIGs. This government-developed product is intended to help System Administrators determine the configuration of a computer and then help them automatically fix most configuration vulnerabilities. Because configuring a system to the DoD

standard can be labor-intensive and prone to error, the potential benefits to the Department are significant.

Public Key Infrastructure (PKI) - Departmental components are accelerating use of Public Key Infrastructure for network access and secure login. Over 3 million personnel are outfitted with Common Access Cards enabling PKI capabilities throughout the Department of Defense population.

We are now implementing PKI-based logon, which will increase the difficulty for adversaries to remotely access Department systems. Upcoming requirements include integrating DoD PKI security services at multiple levels to include DoD websites to lessen the likelihood of unauthorized disclosure of DoD information.

Password Stand-Down – The CIO has emphasized the need to implement CAC/PKI single sign-on to networks. On November 29, 2005 the Joint Task Force-Global Network Operations (JTF-GNO) directed a DoD-wide Network Stand-Down Day to require DoD elements to confirm all accounts and users were required to change passwords or their accounts were locked.

DoD IA Workforce Management - The Department recently published the DoD IA Workforce Improvement Program Manual, DoD 8570.01M, establishing a Department-wide IA standard for IA workforce management and baseline knowledge and skills that all personnel performing IA functions including military, civilians and contractors must meet . This manual leverages industry best practices and raises the bar on IA certifications by requiring they be accredited by

the American National Standards Institute (ANSI) to meet the International Organization for Standardization/International Electro-technical Commission (ISO/IEC) standard 17024, *General Requirements for Bodies Operating Certification of Persons.*

- The DoD IA Scholarship Program (IASP) was established in 2002 to attract and retain top talent and to target academic research to support the mission critical IA/IT needs of the Department. Since its inception, 206 students have been in the DoD IA Scholarship Program (IASP). Through March 2005, 65 have graduated and either are working in DoD or have completed their obligation.
- Instituted the Centers of Academic Excellence in Information Assurance Education program; and expanding it from 23 universities in 21 States in 2002, to 66 universities in 27 States today. These include 4 DoD schools (US Military Academy, US Air Force Academy, Air Force Institute of Technology, and Naval Postgraduate School)

Vulnerability Management Process - DoD is employing an aggressive approach to patch management and vulnerability mitigation across the enterprise. DoD has implemented a process called the Information Assurance Vulnerability Alert (IAVA) Management Program to mandate the rapid application of software patches and configuration changes when security vulnerabilities are identified. The IAVA process requires the Combatant Commands, Services, and Defense agencies to update configurations to incorporate the new patches or to take other

vulnerability remediation actions directed by the JTF-GNO. In turn, Components report their compliance with these security mandates.

While patching and configuring tens of thousands of devices (servers, routers, computers, etc.) can be challenging, DoD has taken significant steps to make configuration change easier and more certain. DISA has established a distribution system for the dissemination of security-relevant patches throughout the enterprise. Patch repositories and antivirus distribution servers are available on the classified and unclassified GIG networks. These repositories enhance DoD's ability to protect against newly announced vulnerabilities because DoD is no longer competing with the entire Internet community for access to vendor-released patches. DoD users have exclusive access to the repositories, thus speeding up the overall response.

Ports, Protocols, and Services - The Department made significant strides in managing network Ports and Protocols. In concert with JTF, the Department established an enterprise program to eliminate unofficial traffic entering and leaving the GIG. These efforts close unused ports, stop the use of vulnerable computer communication protocols that could easily allow hackers to access our systems, and reduces the risk of potentially malicious traffic entering and leaving the Global Information Grid (GIG).

Host (workstations and servers) Vulnerability Scanning and Remediation - In 2005 the DoD purchased and deployed two enterprise software tools that permit system administrators to scan and report compliance with DoD vulnerability patch

policies and push patches to remote machines. These two tools reduce time to patch security holes being exploited by our adversaries and for senior leaders to verify compliance across the Department.

Host Based Security System (HBSS) - HBSS is a host based intrusion prevention system to increase the difficulty for adversaries to compromise DoD hosts. Additionally HBSS permits system administrators to repeatedly baseline their systems and compare baselines to discover changes that indicate adversary activity. HBSS is currently going through source selection and contracting.

Spyware - In July 2005, DISA awarded a contract for a DoD enterprise-wide anti-spyware solution to complement its very successful enterprise anti-viral capability. The solution will be used by System Administrators and cyber-security personnel throughout the Department, including the DoD-related intelligence agencies, the National Guard, and the Reserves.

Enhanced Inspection Program - The Department is increasing the scanning of DoD networks to discover networks in violation of DoD policies; the Department will direct actions to mitigate deficiencies.

Enterprise Intrusion Detection Systems - The Enterprise Solutions Steering Group (ESSG) in coordination with DISA and JTF-GNO is allocating new sensors for DoD components to improve the current DoD enterprise sensor grid and established tighter sensor configurations on backbone networks.

Network Mapping - The JTF-GNO is enabled operations of a DISA automated network mapping capability to improve situational awareness of the DoD enterprise networks.

Incident Handling - The Joint Staff updated incident handling guidance formalizing the current ad hoc processes across the communications, operations, law enforcement, counter-intelligence, and intelligence community. Additionally this policy requires operational commanders and leaders to report incidents impacting mission effectiveness or support of deployed and contingency force operations through operational channels in addition to communications channels.

Information Condition (INFOCON) Policy - The DoD INFOCON policy is an alert and response system designed to permit the Commander, US STRATCOM to assess and respond to enterprise-wide cyber threats.

Status of Information Security and FISMA Implementation in DoD

The Department of Defense uses FISMA as a management and assessment tool to improve its IT security posture. The Defense-wide Information Assurance Office (DIAP) is responsible for oversight of the Information Assurance program for DoD. In addition, the DIAP orchestrates the FISMA process with representatives from all the DoD reporting Components, which include the Military Services, the Combatant Commands, DoD Agencies, and DoD Field Activities.

The Department continues to enhance its FISMA effort consistent with guidance from OMB. Specifically:

- The Department continues to add mission support systems to its reportable inventory and reviewed over 3,500 systems in Fiscal Year 2005 – an increase of more than 1,000 systems from Fiscal Year 2004.
- The Department increased its Authority to Operate (ATO) rate from 58% in Fiscal Year 2004 to 82% in fiscal year 2005. In addition, our total Accreditation rate (ATO/IATO) was 93 percent.
- The Department is including a detailed POA&M process in the FY06 DoD FISMA guidance. These improvements let us better track and analyze systemic issues.
- Last year, more than 2 million of the approximately 2.6 million DoD military, civilian, and contractor personnel who had access to DoD networks received documented IA security awareness training. This training was accomplished even while larger numbers of Service members were deployed to combat theaters. In addition, more than 67,000 individuals with significant security responsibilities received documented specialized security training.
- The DoD IT Portfolio Repository (DITPR) is the database of record for the FISMA system reporting. The OSD uses the DoD IT Portfolio Repository (DITPR) to compile the system metrics of the FISMA report. In accordance with Deputy Chief Information Officer Memorandum December 21, 2004, all Mission Support systems are being entered into the data base by the end of Fiscal year 2006.

Identified Security Weaknesses and Remediation

In the current year FISMA report, the DoD Office of the Inspector General (OIG) identified the following areas as deficient. I will address these areas specifically, and offer our status or remediation effort.

Issue: The OIG has stated that DoD lacks an inventory of major information systems, with identified interfaces, including those not under control of the agency.

Response: We believe the inventory of major information systems under the control of the Department is as accurate as possible considering the dynamic environment and sheer number of systems deployed across the DoD enterprise. We are also continuing the effort to complete a comprehensive enterprise-wide inventory, including mission support systems.

Issue: The IG has stated that the Departmental Plan of Actions and Milestones process is not an agency wide process, incorporating all known IT Security weaknesses.

Response: The Department has developed comprehensive POA&M guidance that has been integrated into the Fiscal Year 2006 DoD FISMA guidance and will be incorporated into a permanent DoD policy issuance in the near future.

Issue: The IG has stated that the quality of DoD Certification and Accreditation (C&A) process is poor and believes that DoD should be following NIST, rather than DoD policy and guidance.

Response: This issue is in the process of being addressed. Section 3543 (c) of FISMA delegates authority to the Secretary of Defense to develop security policies and guidelines for all DoD information systems. The DoD C&A process is currently under

revision. It is consistent with NIST guidelines but it is more extensive and has a somewhat different orientation because it must address classified national security systems as well as the non-national security systems covered by NIST guidelines.

Issue: The IG has stated that the Department is not aware of the number of employees with significant IT Security responsibilities.

Response: The DoD Components reported a total of 79,986 employees with significant IT security responsibilities in FY05. In such a large and dynamic organization, that number will always be in flux. However, in our continued drive for effective workforce management, the Department has established a comprehensive process under the newly issued DoD training and workforce improvement manual to account for and track all IT security personnel and IT security certifications in order to reflect the most accurate number possible.

What are the greatest obstacles to addressing these weaknesses?

Considering the size, complexity, and dynamically changing operational tempo of the Department of Defense, the Office of the CIO considers the greatest obstacles to be keeping up with the asymmetric threat landscape, and our ability to defend the network in an agile manner.

What Additional Guidance, Procedures, or Resources the Department Feels It Needs to Improve Its Information Security and FISMA Compliance?

For large organizations such as the Department of Defense, the FISMA IG review should take the form of an assessment rather than a formal audit. Additional guidance toward this goal can be offered to assist in standardizing IG FISMA assessments across

all federal agencies. Additionally, the dynamic environment of The Department of Defense requires unique policies and procedures.

Conclusion

The Department of Defense is committed to a strong and comprehensive security program. The Department continues to move forward to address enterprise solutions necessary for protecting its information systems and networks. Our commitment to improve our FISMA compliance is an essential element of the Department's information security strategy.

Again, I thank you for the opportunity to comment on this important topic and I look forward to answering any questions you may have.